

# MAPS-EH

## Monitoraggio e Attuazione Policy di Sicurezza nell'eHealth



ATON IT Innovation Technology  
Via Fiume Giallo, 3 – 00144 – Roma



Deep Blue  
Via Daniele Manin, 53 - 00185 Roma

## Cos'è MAPS-EH?

MAPS-EH si occupa di **migliorare** la copertura, l'efficienza, la flessibilità e l'economicità del **monitoraggio dell'attuazione delle policy di sicurezza informatica**

Si pone particolare attenzione all'**ambito dell'eHealth**, dove è fondamentale garantire il **massimo livello di protezione dei dati**

R

CONTENUTO PER GLI ABBONATI PREMIUM

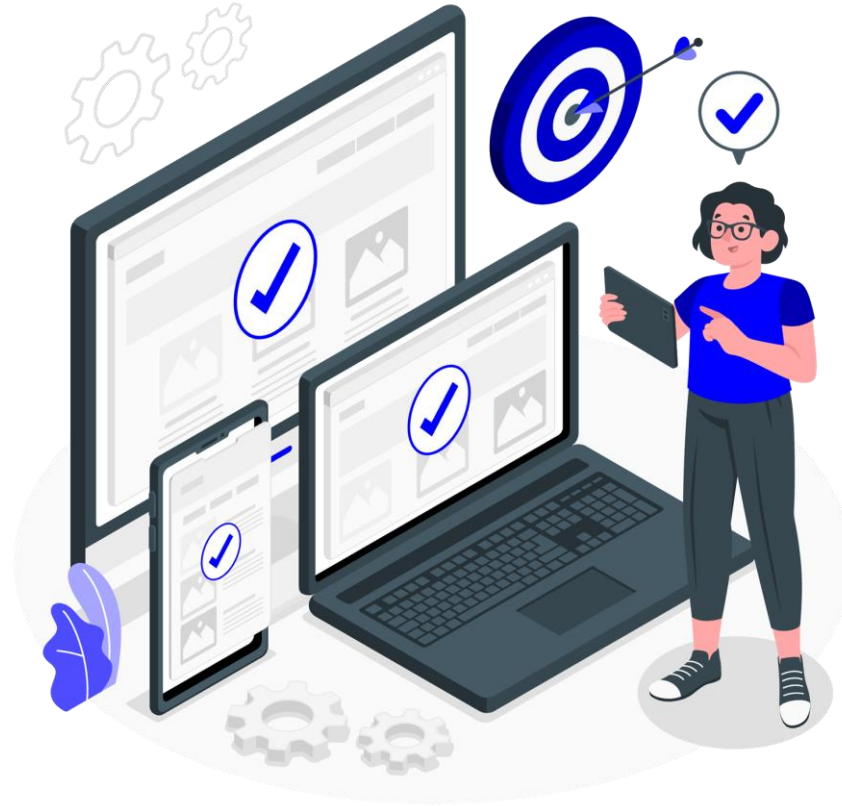
**La sanità sotto ricatto degli hacker: l'Abruzzo paralizzato, i primi dati sensibili in rete. E tra i pazienti c'è Matteo Messina Denaro**

di Michele Bocci, Giuliano Foschini

# Obiettivo

L'obiettivo del progetto è innovare la gestione del processo di monitoraggio dell'allineamento tra "policy e attuazione"

La soluzione prevede un IAM, un SIEM ed una serie di componenti di comunicazione per applicazioni di terze parti



# IAM – Identity and Access Management

Un IAM è uno strumento che definisce chi sono gli utenti che possono accedere a una rete e cosa possono fare, vedere ed usare

Il principio è quello dell'addetto alla sicurezza in aeroporto: il software IAM è la sua versione digitale e si preoccupa di verificare la tua identità e se puoi entrare nel paese

Con l'unica differenza che non solo controlla se puoi entrare in un particolare stato ma anche in quali regioni, province o comuni

In questo modo contribuisce a garantire la protezione e la sicurezza delle persone che vivono al suo interno

WS<sub>2</sub> Identity Server

WS<sub>2</sub> API Manager



# SIEM – Security Information and Event Management

Il SIEM è una soluzione di sicurezza informatica che aiuta le organizzazioni a riconoscere le potenziali minacce e vulnerabilità all'infrastruttura IT prima che si verifichino

Possiamo vederla come una branca che sfrutta i log prodotti dai vari sistemi IT in modo superiore al log management

Utilizza infatti l'intelligenza artificiale per automatizzare molti dei processi manuali associati al riconoscimento delle minacce, alla risposta agli incidenti e all'analisi del comportamento degli utenti per prevedere pericoli incombenti all'infrastruttura IT



# Prevenzione attacchi interni

Il numero di attacchi alle reti aziendali cresce ogni anno, i costi medi associati ad ogni attacco crescono e la maggior parte delle minacce arriva dall'interno (account deboli o dipendenti scontenti)

Quindi diventa fondamentale dotarsi di sistemi di prevenzione e controllo





# Sondaggio!

Partecipa ora a questo breve sondaggio per indagare conoscenze, attitudini e dubbi sul tema della cybersicurezza, al fine di individuare i comportamenti virtuosi o potenziali rischi nelle organizzazioni

Il questionario è del tutto anonimo.  
Grazie!



# Conclusioni

Questo progetto ha consentito ad Aton Informatica e Deep Blue di migliorare le proprie competenze interne nel campo della sicurezza informatica, della gestione dei dati e dei log e degli eventi

Nei prossimi anni, Aton Informatica prevede di ampliare la propria offerta commerciale per fornire soluzioni di sicurezza integrate